WHAT IS CLAIMED IS:

1. A computer-readable medium containing program instructions for configuring a first computer so that a first telephony client on the first computer may securely communicate with a second telephony client on a second computer via a communication path, the computer-readable medium comprising computer code for inserting a security algorithm within the communication path, the security algorithm facilitating secure communication between the first and second telephony clients such that more than a single type of telephony client may be implemented.

2. A computer-readable medium as recited in claim 1, wherein insertion of the security algorithm allows the first telephony client to be different from the second telephony client.

3. A computer-readable medium as recited in claim 1, wherein the security algorithm is inserted within the first computer's operating system kernel.

4. A computer-readable medium as recited in claim 3, wherein the first computer's operating system kernel is in the form of an operating system having an I/O supervisor and a sound class driver, and the security algorithm is inserted between the I/O supervisor and the sound class driver, the security algorithm being configured as a filter driver.

5. A computer-readable medium as recited in claim 3, wherein the security algorithm is selected from a group consisting of an IDEA encryption algorithm, a DES encryption algorithm, a GOST algorithm, an RC5 algorithm, and a SEAL algorithm.

6. A computer-readable medium as recited in claim 1, wherein the security algorithm is not implemented within a user mode of the first computer's operating system.

7. A computer-readable medium as recited in claim 6, wherein the security algorithm is independent from the first or second telephony clients or any codecs or communication stacks used in conjunction with the first or second telephony clients.

8. A method of configuring a first computer so that a first telephony client on the first computer may securely communicate with a second telephony client on a second computer via a communication path, the method comprising inserting a security algorithm within the communication path, the security algorithm facilitating secure communication between the first and second telephony clients such that more than a single type of telephony client may be implemented.

9. A method as recited in claim 8, wherein insertion of the security algorithm allows the first telephony client to be different from the second telephony client.

10. A method as recited in claim 8, wherein the security algorithm is inserted within the first computer's operating system kernel.

11. An operating system for use by a processor in directing operation of a computer upon which a first telephony client may execute to communicate with a second telephony client on a second computer via a communication path, the operating system comprising:

at least one processor-readable medium; and

a program mechanism embedded in the at least one processor-readable medium for causing the processor to facilitate secure communication between the first and second telephony clients such that any combination of types of telephony clients may be implemented.

12. A computer-readable medium containing program instructions for a first telephony system to communicate securely with a second telephony system, the first telephony client being configurable to include a sound card and an associated driver, a general purpose sound driver for interfacing with the sound card's associated driver, a network card and associated driver, a general purpose networking driver for interfacing with the network card's associated driver, a telephony client, an I/O supervisor for interfacing between the telephony client and the general purpose networking and sound drivers, the computer-readable medium comprising:

computer code for inserting a filter driver between the I/O supervisor and the general purpose sound driver,

wherein the filter driver is capable of encrypting audio signals received into the sound card prior to the audio signals being received by the telephony client and transmitted to the network card, and

wherein the filter driver is also capable of decrypting audio signals received by the network card and passed through the telephony client to the filter driver, the decryption occurring prior to transmitting the audio signals to the sound card.

13. A computer-readable medium containing programming instructions for a first telephony client having an associated formatting module to communicate securely with a

second telephony client, the computer-readable medium comprising:

computer code for receiving audio signals from an audio input device;

computer code for encrypting the received audio signals independently of the formatting module associated with the first telephony client; and

computer code for outputting the encrypted audio signals for transmission to the second telephony client.

14. A computer-readable medium as recited in claim 13, wherein the formatting module is configured to compress the audio signals using an algorithm selected from a group consisting of a G.711 codec, a G.723 codec, and a G.729 codec.

15. A computer-readable medium as recited in claim 13, wherein the formatting module is different for different types of telephony clients and the encrypting is independent of telephony client type.

16. A computer-readable medium as recited in claim 15, wherein the first telephony client has a different type than the second telephony client.

17. A computer-readable medium as recited in claim 13, wherein the formatting module is implemented in a sound card driver that is configured to interface with a sound card that receives and outputs audio signals.

18. A computer-readable medium as recited in claim 13, wherein encrypting is also performed independently from a communication stack implemented by the first telephony client.

19. A computer-readable medium as recited in claim 13, wherein encrypting is performed independently from the first telephony client.

20. A computer-readable medium as recited in claim 13, wherein the encrypting implements an algorithm selected from a group consisting of an IDEA encryption algorithm, a DES encryption algorithm, a GOST algorithm, an RC5 algorithm, and a SEAL algorithm.

21. A computer-readable medium containing programming instructions for a first telephony client having an associated interpreting module to communicate securely with a second telephony client, the computer-readable medium comprising:

computer code for receiving audio signals from a network input device;

computer code for decrypting the received audio signals independently of the interpreting module associated with the first telephony client; and

computer code for outputting the decrypted audio signals for transmission to an audio output device.

22. A computer-readable medium as recited in claim 21, wherein the interpreting module is configured to decompress audio signals that are compressed with an algorithm selected from a group consisting of a G.711 codec, a G.723 codec, and a G.729 codec.

23. A computer-readable medium as recited in claim 21, wherein the interpreting module is different for different types of telephony clients and the encrypting is independent of telephony client type.

24. A computer-readable medium as recited in claim 23, wherein the first telephony client has a different type than the second telephony client.

25. A computer-readable medium as recited in claim 21, wherein the interpreting module is implemented in a sound card driver that is configured to interface with a sound card that receives and outputs audio signals.

26. A computer-readable medium as recited in claim 21, wherein decrypting is also performed independently from a communication stack implemented by the first telephony client.

27. A computer-readable medium as recited in claim 21, wherein decrypting is performed independently from the first telephony client.

28. A computer-readable medium as recited in claim 21, wherein the decrypting implements an algorithm selected from a group consisting of an IDEA encryption algorithm, a DES encryption algorithm, a GOST algorithm, an RC5 algorithm, and a SEAL algorithm.

29. A method of transmitting a telephonic signal from a first telephony system to a second telephony system comprising:

initiating a telephonic session between the first and second telephony systems;

formatting a telephonic signal into a predetermined format that is recognizable by the second telephony system, the formatting being performed in response to a telephonic signal received into a telephonic input device of the first telephonic system;

encrypting the telephonic signal with a security algorithm, wherein the encrypting is independent of the formatting; and

transmitting the telephonic signal to the second telephony system after the telephonic signal has been encrypted and formatted.

30. A method of a first telephony system to receive a telephonic signal from a second telephony system comprising:

receiving a telephonic signal from the second telephony system, the received telephonic signal being formatted into a predetermined format by the second telephony system;

interpreting the predetermined format of the telephonic signal received from the second telephony system; and

decrypting the received telephonic signal, the decrypting being performed independently of the interpreting of the predetermined format.

31. A computer system for communicating telephonic signals between a first telephony system and a second telephony system, the computer system comprising:

a formatting module arranged to configure telephonic signals into a first predetermined format that is recognizable by the second telephony system, the formatting being performed in response to a telephonic signal received into a telephonic input device of the first telephonic system;

an interpreter module arranged to recognize a second predetermined format of telephonic signals received from the second telephony system; and

a security module arranged to encrypt telephonic signals prior to transmission to the second telephony system and to decrypt telephonic signals received by the first telephony system, wherein the encrypting is independent of the first predetermined format that is recognizable by the second telephony system and the decryption is independent from the second predetermined format of telephony signals received by the first telephony system.